Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for providing public key infrastructure security in a wide area computer network comprising:

a user terminal coupled to the computer network including a client system;

a private key, and a public key assigned to a user when the user registers with the system using the user terminal;

a database remote from the user terminal for securely storing the private key and the public key in a user transaction data record assigned to the user; and

a server system remote from the user terminal and coupled to the computer network including a computer executable code for ~~performing a cryptographic function as a user transaction data on behalf of the user~~ authenticating the user with the user transaction data record assigned to the user utilizing the stored private key in the database, wherein the private key assigned to the user is not stored in the client system.

2. (Original) The system of claim 1, further comprising a plurality of security device transaction data stored in the database, wherein each security device transaction data is related to a respective user.

3. (Original) The system of claim 1, wherein the private key is encrypted when it is stored in the database.

4. (Currently Amended) The system of claim 2, wherein a respective security device transaction data related to a user is loaded into [[the]] a cryptographic device when the user requests a service.

5. (Original) The system of claim 1, wherein the server system includes a cryptographic device to authenticate the identity of the user and verify that the identified user is authorized to assume a role and perform a corresponding operation.

6. (Original) The system of claim 5, wherein the assumed role is a security officer role to initiate a key management function.

7. (Original) The system of claim 5, wherein the assumed role is an administrator role to manage a user access control database.

8. (Original) The system of claim 5, wherein the assumed role is a provider role to withdraw from a user account.

9. (Original) The system of claim 5, wherein the assumed role is a user role to operate on a value bearing item.

10. (Original) The system of claim 5, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

11. (Original) The system of claim 5, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

12. (Original) The system of claim 5, wherein the cryptographic device stores information about a number of last transactions in a respective internal register.

13. (Original) The system of claim 12, wherein the database stores a table including the respective information about a last transaction, a verification module to compare the information saved in the device with the information saved in the database.

14. (Original) The system of claim 1,further comprising a digital certificate stored in the database and assigned to a user when the user registers with the system.

15. (Original) The system of claim 1, wherein the cryptographic function is digitally signing a certificate.

16. (Original) The system of claim 1, wherein the cryptographic function is encrypting data.

17. (Original) The system of claim 1, wherein the cryptographic function is decrypting data.

18. (Original) The system of claim 1, wherein the database includes a user profile for the user.

19. (Original) The system of claim 18, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period.

20. (Original) The system of claim 5, wherein the cryptographic device is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

21. (Original) The system of claim 5, wherein the cryptographic device stores information about a number of last transactions in an internal register and compares the information saved in the register with the information saved in a memory before loading a new transaction data.

22. (Currently Amended) A method for providing public key infrastructure security in a wide area computer network comprising the steps of:

assigning a private key and a public key ~~certificate~~ to a user when the user registers with the system using a user terminal coupled to the computer network;

storing the private key and the public key in a user transaction data record assigned to the user, in a database remote from the user terminal; and

~~performing a cryptographic function as a user transaction data on behalf of the user utilizing the stored private key~~ authenticating the user with the user transaction data record assigned to the user utilizing the stored private key in the database, wherein the private key assigned to the user is not stored in the client system.

23. (Original) The method of claim 22, further comprising the step of storing a digital certificate and assigning the stored digital certificate to a user when the user registers with the system.

24. (Original) The method of claim 22, further comprising the step of storing a plurality of security device transaction data in the database, wherein each transaction data is related to one of a plurality of users.

25. (Currently Amended) The method of claim 24, further comprising the step of loading a security device transaction data related to a user into one of [[the]] one or more of cryptographic devices when the user requests to operate on a value bearing item.

26. (Original) The method of claim 25, further comprising the step of verifying that the requesting user is authorized to assume a role and to perform a corresponding operation.

27. (Original) The method of claim 26, wherein the assumed role is an administrator role to manage a user access control.

28. (Original) The method of claim 26, wherein the assumed role is a user role to perform expected IBIP postal meter operations.

29. (Original) The method of claim 26, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified.

30. (Original) The method of claim 26, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator.

31. (Currently Amended) The method of claim [[22]] 25, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database;

comparing the information saved in the respective device with the respective information saved in the database; and

loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

32. (Original) The method of claim 22, wherein the cryptographic function is digitally signing a certificate.

33. (Original) The method of claim 22, wherein the cryptographic function is encrypting data.

34. (Original) The method of claim 22, wherein the cryptographic function is decrypting data.

35. (Original) The method of claim 22, further comprising the step of storing a user profile for a plurality of users.

36. (Original) The method of claim 35, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period

37. (Original) The method of claim 22, wherein the cryptographic function is one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.